UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/529,353	03/25/2005	Martin C Rosner	US020357US	2542

24737 7590 10/28/2008

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
OKEKE, IZUNNA	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
10/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/529,353	ROSNER ET AL.	
	Examiner	Art Unit	
	IZUNNA OKEKE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/05/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 08/19/2008 have been fully considered but they are not persuasive.

Applicant argues that the target node of Lundkvist does not communicate a first response to the source node immediately after the query is received. Examiner maintains that Lundkvist teaches the target node communicating a first response to the source node immediately after receiving the query. In Para 32, Lundkvist teaches receiving a first signal X from the source node, the target node decrypts the encrypted signal, then encrypts a first signal Y1 and immediately sends the first encrypted signal Y1 to the source node. The processing which applicant referred to is the encryption of the signal, Y1, which is done in the art to protect the message. Examiner maintains the rejection as being fully anticipated by the prior art of Lundkvist

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action

2. Claims 1-7, 11-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Lundkvist (US-2003/0184431).

a. *Referring to amended claim 1:*

Regarding amended claim 1, Lundkvist teaches a method of determining proximity of a target node to a source node, comprising:

communicating a query from the source node to the target

node (Para 31, Line 8-10 teaches communicating a query from a source to a target device): communicating a first response from the target node to the source node, immediately after the query is received at the target node (Para 32 teaches the target node sending the response Y1 immediately to the source node);

receiving the first response at the source node (Para 32 teaches the source node receiving the first response Y1);

processing the query at the target node to produce therefrom a second response that facilitates a verification of the target node and its first response (Para 34, Line 1-5 teaches a second signal sent from the target device to the source containing verification information);

communicating the second response from the target node to the source node (Para 34, Line 1-5 teaches sending the second response to the source object);

determining a measure of communication time between communicating the query and receiving the first response (Para 32, Line 8-11 teaches measuring a time T1 between sending the first signal and receiving a response); and

determining the proximity of the target node based on the measure of communication time (Para 18, Line 15-18 teaches determining the proximity of the target node based on the measure of communication time).

a. *Referring to claim 2:*

Regarding claim 2, Lundkvist teaches the method of claim 1, wherein the query and at least one of the first and second responses correspond to at least a portion of a cryptographic key-exchange protocol (Para 29, 31 and 32 teaches the information

including the query and the 1st and 2nd responses exchanged between the object and the device corresponds to a cryptographic key-exchange protocol such as asymmetric key pair cryptography).

a. *Referring to claim 3:*

Regarding claim 3, Lundkvist teaches the method of claim 2, wherein the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol (Para 29, Line 12-14 teaches a symmetric key encryption which is a type of Needham-Schroeder protocol can be used in the key exchange).

a. *Referring to claim 4:*

Regarding claim 4, Lundkvist teaches the method of claim 1, wherein the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol (Para 29 - 34 teaches the first and second response corresponding to an authentication stage, a key exchange stage, a key generation phase and a data transmission phase of the OCPS protocol).

a. *Referring to claim 5:*

Regarding claim 5, Lundkvist teaches the method of claim 1, wherein the query includes an encryption of an item based on a public key of the target node (Para 29 and Para 31 teaches the encrypting identity information and the random number based on asymmetric key pair cryptography such as the public key of the target node), and the processing of the query includes decrypting the item based on a private key of the target node, for inclusion in the second response (Para 29 and Para 32 teaches the portable unit decrypting the item based on asymmetric key pair cryptography).

a. *Referring to claim 6:*

Regarding claim 6, Lundkvist teaches the method of claim 5, wherein the first response includes a random number, and the processing of the query further includes encrypting the item and the random number using a public key of the source node to form at least a portion of the second response (Para 32, line 1-7 teaches the first response comprising the first information which includes a random number and Para 29 teaches encryption of all responses sent between the nodes. Para 34 the second response Y2 being a function of the first response which includes the random number and the object ID).

a. *Referring to claim 7:*

Regarding claim 7, Lundkvist teaches the method of claim 5, wherein the first response includes an encryption of a random number based on a public key of the source node (Para 32, Line 1-6 teaches the first response Y1 as an encrypted signal comprising the first information which consists of a random number).

a. *Referring to amended claim 11:*

Regarding amended claim 11, Lundkvist teaches a node on a network including: a communication device that is configured to receive a query from a source node and to transmit a first response that facilitates proximity verification of the node, to the source node immediately upon receipt of the query, and a second response that facilitates a verification of the node to the source node (See the rejection in claim 1 and Para 30-34), and

a processor that is configured to process the query and produce therefrom the second response (Para 322 teaches the portable unit as a processor to process the query sent from the object).

a. *Referring to claim 12:*

Regarding claim 12, Lundkvist teaches the node of claim 11, wherein the processor is configured to process the query and produce the response as part of a cryptographic key-exchange protocol (Para 29, 31 and 32 teaches the information including the query and the 1st and 2nd responses exchanged between the object and the device corresponds to a cryptographic key-exchange protocol such as asymmetric key pair cryptography).

a. *Referring to claim 13:*

Regarding claim 13, Lundkvist teaches the node of claim 12, wherein the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol (Para 29, Line 12-14 teaches a symmetric key encryption which is a type of Needham-Schroeder protocol can be used in the key exchange).

a. *Referring to claim 14:*

Regarding claim 14, Lundkvist teaches the node of claim 11, wherein the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol initiated by the source node (See the rejection to claim 4).

a. *Referring to claim 15:*

Regarding claim 15, Lundkvist teaches the node of claim 11, wherein the query includes an encryption of an item based on a public key of the node (Para 29 and Para

31 teaches the encrypting identity information and the random number based on asymmetric key pair cryptography such as the public key of the target node), and

the processor is configured to decrypt the item based on a private key of the node, for inclusion in the second response. (Para 29 and Para 32 teaches the portable unit decrypting the item based on asymmetric key pair cryptography)

a. *Referring to claim 16:*

Regarding claim 16, Lundkvist teaches the node of claim 15, wherein the first response includes a random number, and the processor is configured to encrypt the item and the random number using a public key of the source node to form at least a portion of the second response (Para 32, line 1-7 teaches the first response comprising the first information which includes a random number and Para 29 teaches encryption of all responses sent between the nodes. Para 34 the second response Y2 being a function of the first response which includes the random number and the object ID).

a. *Referring to claim 17:*

Regarding claim 17, Lundkvist teaches the node of claim 15, wherein the first response includes an encryption of a random number based on a public key of the source node (Para 32, Line 1-6 teaches the first response Y1 as an encrypted signal comprising the first information which consists of a random number).

a. *Referring to amended claim 18:*

Regarding amended claim 18, Lundkvist teaches a node on a network including: a communication device that is configured to transmit a query to a target node and to receive an immediate first response and a second response from the target node (See

the rejection in claim 1 about immediately sending a first response and Para 31 teaches the control unit of the transmitting a first query to the target device and receiving a 1st and 2nd response); and

a processor that is configured to: measure a communication time between transmitting the query and receiving the first response (Para 32, Line 8-14 teaches the control unit measuring a communication time between the first transmission and the first response), determine a proximity of the target node relative to the node based on the communication time, and verify the target node based on the second response (Para 34 teaches the control unit determining the proximity of the target node and verifying the target node based on the decrypted second response).

a. *Referring to claim 19:*

Regarding claim 19, Lundkvist teaches the node of claim 18, wherein the processor is configured to generate the query and process at least one of the first and second responses as part of a cryptographic key-exchange protocol (See Para 31 and 34).

a. *Referring to claim 20:*

Regarding claim 20, Lundkvist teaches the node of claim 19, wherein the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol (Para 29, Line 12-14 teaches a symmetric key encryption which is a type of Needham-Schroeder protocol can be used in the key exchange).

a. *Referring to claim 21:*

Regarding claim 21, the combination of Lundkvist and Davis teaches the node of claim 18, wherein the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol initiated by the node (See the rejection to claim 4).

a. *Referring to claim 22:*

Regarding claim 22, Lundkvist teaches the node of claim 18, wherein the query includes an encryption of an item based on a public key of the target node (Para 29 and Para 31 teaches the encrypting identity information and the random number based on asymmetric key pair cryptography such as the public key of the target node), and the second response includes a decryption of the item based on a private key of the target node (Para 29 and Para 32 teaches the portable unit decrypting the item based on asymmetric key pair cryptography).

a. *Referring to claim 23:*

Regarding claim 23, Lundkvist teaches the node of claim 22, wherein the first response includes a random number, and the second response includes an encryption of the decryption of the item and the random number, using a public key of the node (Para 32, line 1-7 teaches the first response comprising the first information which includes a random number and Para 29 teaches encryption of all responses sent between the nodes. Para 34 the second response Y2 being a function of the first response which includes the random number and the object ID).

a. *Referring to claim 24:*

Regarding claim 24, Lundkvist teaches the node of claim 23, wherein the second response further includes a signature of the decryption of the item and the random number, using a private key of the target node (Para 34, line 7-10 teaches a second response Y2 which includes an encryption of a random number based on a public key of the node).

a. *Referring to claim 25:*

Regarding claim 25, Lundkvist teaches the node of claim 22, wherein the first response includes an encryption of a random number based on a public key of the node (Para 32, Line 1-6 teaches the first response Y1 as an encrypted signal comprising the first information which consists of a random number).

Claim Rejections - 35 USC § 103

3. Claims 8-10, 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lundkvist (US-2003/0184431), and further in view of Davis et al. (US-6088450).

a. *Referring to claim 8:*

Regarding claim 8, Lundkvist teaches the method of claim 1, wherein determining the proximity includes comparing the communication time to a threshold value.

Lundkvist does not teach distinguishing between local and remote nodes based on the proximity.

However, Davis teaches distinguishing between local and remote nodes based on the proximity (See Davis, Col 4, Line 2-11 teaches distinguishing between local and remote nodes by determining when a device is within the proximity level).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to modify Lundkvist's system to be used in a network to determine local and remote nodes as taught by Davis for the purpose of providing security for the network by allowing access to resources within a specified boundary and limiting access to sources outside the boundary

a. *Referring to claim 9:*

Regarding claim 9, the combination of Lundkvist and Davis teaches the method of claim 1, further including restricting communications with the target node based on the proximity (See Davis, Col 4, Line 2-11 teaches prohibiting communications with nodes outside of the proximity perimeter).

a. *Referring to claim 10:*

Regarding claim 10, the combination of Lundkvist and Davis teaches the method of claim 1, further including restricting access of the target node to system resources based on the proximity (See Davis, Col 4, Line 2-11 teaches prohibiting access to resources from nodes outside of the proximity perimeter).

a. *Referring to claim 26:*

Regarding claim 26, the combination of Lundkvist and Davis teaches the node of claim 18, wherein the processor is configured to determine the proximity based on a comparison of the communication time to a threshold value that distinguishes between local and remote nodes (See the rejection to claim 8).

a. *Referring to claim 27:*

Regarding claim 27, the combination of Lundkvist and Davis teaches the node of claim 18, wherein the processor is further configured to control subsequent communications with the target node based on the proximity (See the rejection to claim 9).

a. *Referring to claim 28:*

Regarding claim 28, the combination of Lundkvist and Davis teaches the node of claim 18, wherein the processor is further configured to control access of the target node to system resources based on the proximity (See the rejection to claim 10).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IZUNNA OKEKE whose telephone number is (571)270-3854. The examiner can normally be reached on 9:00am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. O./
Examiner, Art Unit 2432

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432